UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/671,058	09/25/2003	Janice Marie Girouard	AUS920030637US1	5828

34533 7590 01/25/2008

INTERNATIONAL CORP (BLF)
c/o BIGGERS & OHANIAN, LLP
P.O. BOX 1469
AUSTIN, TX 78767-1469

EXAMINER	
SHAN, APRIL YING	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
01/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/671,058
Filing Date: September 25, 2003
Appellant(s): GIROUARD ET AL.

John R. Biggers (Reg. 44,537)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 10/30/2007 appealing from the Office action mailed 5/31/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6996718	Henry et al.	2-2006
7085933	Challener et al.	8-2006
6625649	D'Souza et al.	9-2003

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-3, 5-6, 8-10, 12-13,15-17 and 19-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Henry et al. (U.S. Patent No. 6,996,718).

As per **claims 1 and 8**, Henry et al. discloses a method/system for providing a password to an application, the method/system comprising:

receiving, from a user, an passkey event ("1. Input account username and 2. Input account location" in fig. 7. Please note input account username and account location corresponds to Applicant's passkey event) uniquely associated with (Please note account user name/account location is a passkey event uniquely associated with one of a plurality of application requiring a password since "**The user id and**

the server name cooperate to uniquely define a unique account belonging to the user" – e.g. col. 4, lines 18-20) one of a plurality of applications ("multiple accounts" – e.g. abstract requiring a password ("3. input common password" in fig. 7)

receiving, from a user, a same master password ("a common password 30" in fig. 1 and col. 3, line 7. Please note a common password corresponds to Applicant's a same master password) for access to each of the plurality of applications ("multiple accounts 40, 50, 60 and 70" in fig. 1 and col. 3, line 8. Please note multiple accounts correspond to Applicant's plurality of applications, e.g. col. 6, lines 40-44 and step 3 fig. 7);

applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password ("A designated password for each account is generated by a hash function of the common password and some account-dependent information" – e.g. abstract. Please note a designated password corresponds to Applicant's an application specific password. "In the present invention, to generate, process and validate the common password and associated designated passwords for each of a user's accounts, a password transform algorithm is utilized. In a preferred embodiment of the present invention, the password transform algorithm may be generalized as follows: pd = Text(Hash(Ui + Pc + Si + Nr)), where, Pd stands for a designated password, Ui for a user ID..Pc for a common password... Si for a server name (such as the server name or URL of the user's account service provider), and Nr for a random number..the Hash () portion represents the hash function..The account-

dependent information includes a user ID, a server name that indicates the account location, and a random number that is associated with the account and stored at the server..**The user id and the server name cooperate to uniquely define a unique account belonging to the user**" – e.g. col. 3, l. 60- col. 4, l. 20); and

submitting the application specific password to the application for access by the user ("The hash value is calculated at the user's computer, and then submitted as a designated password to a server" – e.g. abstract and "Once a user's account has been established as discussed above, the user will be able to access his/her account at the server...and the server prompts the user to submit the designated password Pd, step 220...The designated password Pd is calculated according to the password transform algorithm, and submitted to the server over the secure connection by the user, step 260..If a match is found, the user is admitted to the account step 280" – e.g. col. 5, lines 24-46 and steps 260-280 in fig. 3).

As per **claims 2 and 9**, Henry et al. discloses a method/system as applied in claims 1 and 8. Henry et al. further discloses wherein applying a hashing algorithm associated with the passkey event to the same master password to generate an application specific password comprises:

retrieving a hash value ("Nr for a random number" – e.g. col. 4, lines 6-7. Please note a random number corresponds to Applicant's hash value) associated with the

passkey event ("a random number that is associated with the account and stored at the server" – e.g. col. 4, lines 15-17); and

applying the hash value to at least one character of the same master password to generate at least one hashed character (col. 3, line 66 and col. 4, lines 1-20. Please note Hash (Ui+Pc+Si+Nr) in col. 3, line 65 corresponds to Applicant's hashed character).

As per **claims 3 and 10**, Henry et al. discloses a method/system as applied in claims 2 and 9. Henry et al. further discloses wherein retrieving a hash value associated with the passkey event comprises retrieving hash value from a user's configuration file (col. 5, lines 29-31).

As per **claims 5 and 12**, Henry et al. discloses a method/system as applied in claims 2 and 9. Col. 3, line 66 and col. 4, lines 1-31 of Henry et al. further discloses wherein applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

retrieving a character rule algorithm; and

applying the character rule algorithm to the hashed character to generate a character rule compliant hashed character.

(Please note according to Applicant's specification page 15-16, Applicant's definition on a character rule algorithm is inclusive with the definition of a master rule

algorithm. Therefore, the cited reference in Henry et al. met the limitations in claims 5 and 12).

As per **claims 6 and 13**, Henry et al. discloses a method/system as applied in claims 3 and 10. Col. 3, line 66 and col. 4, lines 1-31 of Henry et al. further discloses wherein applying a hashing algorithm associated with the passkey event to the master password to generate an application specific password comprises:

retrieving a master rule algorithm; and

applying the master rule algorithm.

(Please note according to Applicant's specification page 15-16, Applicant's definition on a character rule algorithm is inclusive with the definition of a master rule algorithm. Therefore, the cited reference in Henry et al. met the limitations in claims 6 and 13).

As per **claims 15-17 and 19-20**, Henry et al. discloses the claimed method of steps as applied above in claims 1-3 and 5-6. Therefore, Henry et al. discloses the claimed computer program product embodied in a record medium for carrying out the method of steps.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 4, 11 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Henry et al. as applied to claims 1-3, 5-6, 8-10, 12-13 and 15-20 above, and further in view of Challener et al. (U.S. Patent No. 7,085,933)

As per **claims 4 and 11**, Henry et al. does not disclose expressly wherein retrieving a hash value associated with the passkey event comprises retrieving a hash value from a configuration register.

Challener et al. discloses wherein retrieving a hash value associated with the passkey event comprises retrieving a hash value from a configuration register (col. 3, lines 1-11).

Henry et al. and Challener et al. are analogous art because they are from the same field of endeavor system and method for improving computer system security.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to incorporate Challener et al.'s retrieving a hash value associated with the passkey event comprises retrieving a hash value from a configuration register into Henry et al.'s method/system.

The motivation of doing so would have been "for a computer system to have trusted computing platform capabilities" and "the random data withheld from caching to disk and from exposure by the secure virtual machine", as taught by Challener et al. (col. 2, lines 53-56 and col. 3, lines 1-11)

As per **claim 18**, the combined teachings of Henry et al. and Challener et al. disclose the claimed method of step as applied above in claim 4. Therefore, the combined teachings of Henry et al. and Challener et al. discloses the claimed computer program product embodied in a record medium for carrying out the method of steps.

7. Claims 7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Henry et al. as applied to claims 1-3, 5-6, 8-10, 12-13 and 15-20 above, and further in view of D'Souza et al. (U.S. Patent No. 6,625,649).

As per **claims 7 and 14**, Henry et al. does not disclose expressly wherein receiving, from a user, a passkey event uniquely associated with any given one of the plurality of applications comprises receiving, from a user, an event created by a user's engaging a keyboard key.

However, D'Souza et al. discloses receiving, from a user, a passkey event uniquely associated with any given one of the plurality of applications comprises receiving, from a user, an event created by a user's engaging a keyboard key, "The technique allows a user to launch specific software applications by simply depressing keys on a keyboard...The keys associated with the applications may be dedicated keys on a conventional keyboard. By depressing the dedicated key, the user may not only launch a software application, but may log onto a network, such as the worldwide web or the Internet, and may directly access a desired website...Where desired, specific combinations of keystrokes may be provided for launching the applications, logging onto a network, accessing specific suites, and so forth...The keyboard includes a plurality of keys for accessing specific Internet or network sites..." – e.g. col. 2, line 26 – col. 3, line 3.

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate D'Souza et al.'s an event created by a user's engaging a keyboard key into Henry's system/method. The motivation of doing so would have been

"a need..for an improved technique for launching applications in a computer system, particularly applications related to launching, logging on, and navigating through computer networks. There is a particular need for a simple and straightforward, user-friendly system for rapidly access such applications..", as disclosed by D'Souza et al. (e.g. col. 2, lines 14-24).

(10) Response to Argument

So that the reader could more easily follow appellant's arguments and the examiner's traversals, the examiner will use the same heading as appellant in responding to appellant's arguments.

Argument Regarding The First Ground Of Rejection On Appeal: Claims 1-3, 5-6, 8-10, 12-13, 15-17, and 19-20 Are Rejected Under 35 U.S.C. 102(e) As Being Anticipated By Henry, Et Al. and Henry Does not Disclose Receiving, From A user, A Passkey Event Uniquely Associated With One of A Plurality Of Applications Requiring A Password

In re pages 5-7, claim 1, appellant argues, "Henry does not disclose a passkey event as claimed here. A passkey event as defined in Applicants original specification at page 10, lines 26-27, is "an event received by an operating system that is created by a user's invoking a passkey." **A passkey may be a designated key on a keyboard, buttons of a mouse, special hardware tokens, or any other input device.** Henry does not disclose a passkey event that is created by a user's invoking such a passkey". "...Neither Henry's user screen for a password transform calculator nor Henry's user

identification and server name cooperating to define a user account discloses receiving, from a user, a passkey event uniquely associated with one of a plurality of applications requiring a password as claimed in the presentation". "Moveover, the passkey events as claimed here is associated with one of a plurality of applications requiring a password. Henry does not disclose applications requiring a password but instead only discloses Web-based accounts requiring a password...Henry's Web-based accounts are not applications as claimed here and as such Henry does not disclose applications requiring a password".

In response the examiner respectfully disagrees. The examiner respectfully points out in the original specification, the Appellant broadly defines "A passkey event is an event received by an operating system that is created by a user's invoking a passkey 201. While the passkey 201 of Figure 2 is a designated key a keyboard, a passkey can be [can be] any input devices such as one or **more keys of a keyboard,** buttons of a mouse, special hardware tokens, or any other input device..." (Specification, page 10, lines 26-27 – page 11, lines 1-3). Comparing to Appellant's argument above, the examiner assumes that the Appellant unintentionally omitted a passkey can be **more keys of a keyboard** in the above argument. However, because a passkey can be **more keys of a keyboard** as disclosed in the specification, Henry et al. met the limitation of passkey event by disclosing in fig. 7 "1. Input account username - luo and 2. Input account location – research.att.com" since users invoke more keys of a keyboard to enter "luo" and "research.att.com". Therefore, "luo" and "research.att.com" are a passkey event uniquely associated with one of a plurality of application requiring a

password since "**The user id and the server name cooperate to uniquely define a unique account belonging to the user**" – Henry et al. col. 4, lines 18-20.

Clearly, the definition of "applications" in the claim is the issue since the Appellant argues that applications as claimed and accounts as disclosed by Henry et al. are different. Since the term is not defined in the claims and the examiner looks to the specification for guidance. The Appellants do not expressly defined the term "applications" in the specification, instead, the Appellants broadly disclose on page 7 of the specification "The present invention is described to a large extent...for providing a password to an application. Persons skilled in the art, however, will recognize that any computer system that includes suitable programming means for operating in accordance with the disclosed methods also falls well within the scope the present invention. Suitable programming means include any means for directing a computer system to execute...." (Specification, page 7) and further in page 8 of the Appellant's specification "...Figure 1 sets forth a block diagram of automated computing machinery useful in providing a password to an application in accordance with various embodiments of the present invention....The term "computer" therefore includes not only general purposes computers such as laptops, personal computer...but also includes devices such as ...PDAs, **network enabled handheld devices**, **internet-enabled mobile telephones,** and so on. (Specification, page 8) and furthermore, the Appellant disclosed on pages 8-9 of the specification "The example computer 106 of Figure 1 includes...**email servers and email clients**....wired-dial-up connections, Ethernet (IEEE 802.3) adapters for wire LAN connections, and 802.11b adapters for

wireless LAN connections". From the above passages, one with ordinary skill in the art at the time of the invention was made would have understood "applications" includes accounts, programs, services, products and information designed for end users to access, such as email applications, electronic commerce sites with product information and etc. In col. 1, lines 11 - 26, Henry et al. discloses "...access to multiple Web-based accounts...**electronic mail accounts**..." Further, Henry et al. discloses in col. 5, lines 24-25, "Once a user's account has been established as discussed above, **the user will be able to access his/her account at the server". Thus, just because Henry et al. does not use the term "application" does not mean accounts, programs, services, applications, products or information could not be interpreted as application.**

Therefore, Henry et al.'s receiving, from a user, a passkey event ("a user's input account name - luo and input account location – research.att.com" received by an operating system that is created by a user's invoking more keys of a keyboard (users invoke more keys of a keyboard to enter "luo" and "research.att.com") uniquely associated with ("**The user id and the server name cooperate to uniquely define a unique account belonging to the user**" – Henry et al., col. 4, lines 18-20) with one of ("any of the user's accounts" – e.g. Henry et al., abstract) a plurality of applications ("...multiple accounts protected by passwords" - Henry et al., abstract) requiring a password ("According to the present invention, a user only needs to remember a common password to access any of the user's accounts. A designated password for each account is generated... - Henry et al., abstract" and "3. input common password" and 4. Get designated password" – Henry et al. fig. 7) **anticipates** Receiving, From A

user, A Passkey Event Uniquely Associated With One of A Plurality Of Applications Requiring A Password as claimed.

Henry Does Not Disclose Applying A Hashing Algorithm Associated With The Passkey Event To The Master Password To Generate An Application Specific Password

In re pages 8, claim 1, appellant argues, "Henry does not disclose, however, at this reference point, or anywhere else in Henry, a passkey event as claimed in the present application and, as such, Henry cannot disclose a hashing algorithm associated with such a passkey event". "Henry does not disclose therefore applying a hash algorithm associated with the passkey event to the master password to generate an application specific password as claimed in the present application".

In response, the examiner respectfully disagrees. First, examiner again respectfully points out in the original specification, the Appellant broadly defines "A passkey event is an event received by an operating system that is created by a user's invoking a passkey 201. While the passkey 201 of Figure 2 is a designated key a keyboard, a passkey can be [can be] any input devices such as one or **more keys of a keyboard,** buttons of a mouse, special hardware tokens, or any other input device..." (Specification, page 10, lines 26-27 – page 11, lines 1-3). Because a passkey can be **more keys of a keyboard** as disclosed in the specification, Henry et al. met the limitation of passkey event by disclosing ("a

user's input account name - luo and input account location – research.att.com" in fig. 7 received by an operating system that is created by a user's invoking more keys of a keyboard (users invoke more keys of a keyboard to enter "luo" and "research.att.com").

Henry et al. additionally discloses "A **designated password for each account** is generated by a **hash function of the common password and some account-dependent information**" – e.g. abstract. Please note a designated password corresponds to Applicant's an application specific password. "In the present invention, to generate, process and validate the common password and associated designated passwords for each of a user's accounts, **a password transform algorithm** is utilized. In a preferred embodiment of the present invention, the password transform algorithm may be generalized as follows: pd = Text(Hash(Ui + Pc + Si + Nr)), where, **Pd stands for a designated password**, **Ui for a user ID**..**Pc for a common password**...**Si for a server name** (such as the server name or URL of the user's account service provider), and Nr for a random number..**the Hash () portion represents the hash function**..**The account-dependent information includes a user ID, a server name that indicates the account location**, and a random number that is associated with the account and stored at the server..**The user id and the server name cooperate to uniquely define a unique account belonging to the user**" – e.g. col. 3, l. 60- col. 4, l. 20).

Thus, Henry et al. anticipates "Applying A Hashing Algorithm Associated With The Passkey Event To The Master Password To Generate An Application Specific Password" as claimed.

Relations Among Claims

In re page 9, claims 8 and 15, appellant argues, "....As explained above in detail, Henry does not disclose a method for providing a password to an application. Therefore, for the same reason that Henry does not disclose a method for providing a password to an application, Henry also does not disclose systems and computer programs products for providing a password to an application corresponding to independent claims 8 and 15. Independent claims 8 and 15 are therefore patentable and should be allowed". "Claims 2-7, 9-14 and 16-20 depend respectively from independent claims 1, 8 and 15...Because Henry does not disclose each and every element of the independent claims, Henry does not disclose each and every element of the dependent claims of the present application. As such, claims 2-7, 9-14, and 16-20 are also patentable and should be allowed".

In response the examiner respectfully disagrees. Appellant's argument for claim 1 as discussed above is traversed and therefore, the same argument for claims 8 and 15 are traversed. Further, Appellant's argument for claims 2-7, 9-14 and 16-20 are based on dependency on claims 1, 8 and 15 and are traversed because argument for claims 1, 8 and 15 are traversed.

In re pages 9-10, claim 5, appellant argues "Consider the second element of dependent claim 5 as an example...Henry's password transform algorithm does not

disclose the second element of claim 5 of the present application because Henry's password transform algorithm is not a character rule algorithm used to generate a character rule algorithm used to generate a character rule compliant hashed character. For precisely similar reasons... and limitation of the dependent claims of the present application Henry does not **anticipate** the dependent claims and the **rejections under 35 U.S.C 103(a)** should be withdrawn".

In response the examiner disagree with this conclusion. First, as argued on page 10 by the Appellants, "and limitation of the dependent claims of the present application Henry does not **anticipate** the dependent claims and the rejections under **35 U.S.C 103(a)** should be withdrawn" should be and limitation of the dependent claims of the present application Henry does not anticipate the dependent claims and the **rejections under 35 U.S.C 102 (e)** should be withdrawn" and the examiner consider this as an unintentional mistake. Second, the examiner respectfully points out the Appellants only presented arguments for dependent claim 5 and therefore, it is not reasonable to reach a conclusion such as "For precisely similar reasons, Henry does not disclose any of the other elements of the dependent claims in the present claim" Third, as broadly defined by the Appellants, "A character rule algorithm therefore, is an algorithm designed to convert the value of the hashed character to a value that is compliant with the password protected application's character rules" (See specification, page 16). In col. 4, lines 21-31, Henry et al. discloses "The second step is to **convert the output of a hash function**, which is usually in binary form, into texts for use as a designated password. If **an account allows Roman letters appear in the password, the BASE64 [BASE64]**

algorithm is used, without ending '=' or '=' in case the total number of bits of a hash value is not a multiple of 24. **If the account only accepts digits, such as a Personal Identification Number (PIN), every 3 bits is converted into a digit....".** Thus, the BASE64[BASE64] algorithm and every 3 bits is converted into a digit of Henry's clearly anticipates Appellant's character rule algorithm used to generate a character rule compliant hashed character and an account allows Roman letters in the password and the only accepts digits clearly anticipate Appellant's password protected application's character rules.

Argument Regarding The Second Ground Of Rejection On Appeal: Claims 4, 11 And 18 Are Rejected Under 35 U.S.C. 103 (a) As Being Obvious Over Henry, Et Al In View Of Challener Et Al (U.S. Patent No. 7,085,933)

In re page 10, claims 4, 11 and 18, appellant argues, "...As shown above, Henry in fact does not disclose each and every element of independent claims 1, 8 and 15. Because Henry does not disclose each and every element of independent claims 1, 8 and 15, the combination of Henry and Challener cannot possibly disclose each and every element of dependent claims 4, 11 and 18...".

In response the examiner respectfully disagrees. Appellant's arguments for claims 1, 8 and 15 as discussed above are traversed. Therefore, Appellant's arguments for claims 4, 11 and 18 are based on dependency on claims 1, 8 and 15 are also traversed.

Argument Regarding The Second Ground Of Rejection On Appeal: Claims 7 And 14 Are Rejected Under 35 U.S.C. 103 (a) As Being Obvious Over Henry, Et Al. In View Of D'Souza Et Al. (U.S. Patent No. 6,625,649).

In re pages 10-11, claims 7 and 14, appellant argues, ""...As shown above, Henry in fact does not disclose each and every element of independent claims 1 and 8. Because Henry does not disclose each and every element of independent claims 1 and 8, the combination of Henry and D'Souza cannot possibly disclose each and every element of dependent claims 7 and 14."

In response the examiner respectfully disagrees. Appellant's arguments for claims 1 and 8 as discussed above are traversed. Therefore, Appellant's arguments for claims 7 and 14 are based on dependency on claims 1, 8 and 15 are also traversed.

Conclusion Of Appellant's Argument

In re pages 11-12, "claims 1-3, 5-6, 8-10, 12-13, 15-17 and 19-20...Henry does not anticipate Applicant's claims". "Claims 4, 11 and 18...The combination of Henry and Challener does not teach or suggest each and every element of Applicants' claims...". "Claims 7 and 14...The combination of Henry and D'Souza does not teach or suggest each and every element of Applicants' claims...".

In response the examiner fails to agree with this conclusion because all the arguments are traversed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

April Y. Shan

/April Y. Shan/

Patent Examiner, Art Unit 2135

KIM VU
PATENT EXAM

Conferees:

Kim Vu (SPE)

Hosuk Song (Primary Examiner)

HOSUK SONG
PRIMARY EXAMINER